Call for Justice, LLC—United Way 2-1-1 Training Paper
Session 12: Identity Theft and Work of the Minnesota Attorney General
May 16 and 17, 2013: Lindsay LaVoie and Jason Hafemann of the Minnesota Attorney General's Office

Featured Speakers' Topic

This month, Lindsay LaVoie and Jason Hafemann with the Minnesota Attorney General's Office will discuss identity theft and resources for callers who believe they've been victimized. Additionally, they will help us to understand what resources the Attorney General's Office offers to persons in need.

What is Identity Theft?

Identity theft occurs when someone uses an individual's personal data without permission to receive some kind of benefit, most commonly money and property. Personal data may also be used by an imposter to fraudulently obtain employment, housing, medical care, utility services, education or to avoid a record of arrest or conviction. Sometimes the theft occurs with stealing a credit card but usually it's far more complex than simple credit card theft.

"Personal data" includes date of birth, gender, address, education, medical history and financial information.

Identity theft is made much easier because of the "personalization" of individuals' personal data by companies that market that data to users. Technology permits various businesses to cheaply gather information about consumers (information gleaned from internet or debit card sales records, medical records, or income records). Those companies then sell that information to other businesses. This is sometimes called "data mining." This compressed data, or bits of it, can sometimes be stolen or misused, which allows for others to misappropriate the data.

Sources such as the non-profit Identity Theft Resource Center sub-divide identity theft into five categories:

- Identity cloning (using another's information to assume his or her identity in daily life)
- Criminal identity theft (posing as another person when apprehended for a crime)
- Synthetic and Financial identity theft (using another's identity information to create either a new identity or to obtain credit, goods and services in another person's name)
- Medical identity theft (using another's identity to obtain medical care or drugs)
- Child identity theft.

Identity theft may be used to facilitate or fund other crimes including illegal immigration, terrorism, phishing and espionage. There are cases of identity cloning to attack payment systems, including online credit card processing and medical insurance.

Identity Cloning and Concealment

In this situation, the identity thief impersonates someone else in order to conceal their own true identity. Examples might be undocumented immigrants, people hiding from creditors or other individuals, or those who simply want to become "anonymous" for personal reasons. Another example is *posers*, a label given to people who use somebody else's photos and information through social networking sites. Mostly, posers create believable stories involving friends of the real person they are imitating. Unlike identity theft used to obtain credit which usually comes to light when the debts mount, concealment may continue indefinitely without being detected, particularly if the identity thief is able to obtain false credentials in order to pass various authentication tests in everyday life.

Criminal Identity Theft

When a criminal fraudulently identifies himself to police as another individual at the point of arrest, it is sometimes referred to as "Criminal Identity Theft." In some cases criminals have previously obtained state-issued identity documents using credentials stolen from others, or have simply presented fake ID. Provided the subterfuge works, charges may be placed under the victim's name, letting the criminal off the hook. Victims might only learn of such incidents by chance, for example by receiving court summons, discovering their drivers licenses are suspended when stopped for minor traffic violations, or through background checks performed for employment purposes.

It can be difficult for the victim of a criminal identity theft to clear their record. The steps required to clear the victim's incorrect criminal record depend on what jurisdiction the crime occurred in and whether the true identity of the criminal can be determined. The victim might need to locate the original arresting officers and prove their own identity by some reliable means such as fingerprinting or DNA fingerprinting, and may need to go to a court hearing to be cleared of the charges. Obtaining an expungement of court records may also be required.

Synthetic and Financial Identity Theft

A variation of identity theft which has recently become more common is *synthetic identity theft*, in which identities are completely or partially fabricated. The most common technique involves combining a real social security number with a name and birthdate other than the ones associated with the number. Synthetic identity theft is more difficult to track as it doesn't show on either person's credit report directly, but may appear as an entirely new file in the credit bureau or as a subfile on one of the victim's credit reports. Synthetic identity theft primarily harms the creditors who unwittingly grant the fraudsters credit. Individual victims can be

affected if their names become confused with the synthetic identities, or if negative information in their subfiles impacts their credit ratings.

Medical Identity Theft

Medical identity theft occurs when someone seeks medical care under the identity of another person. In addition to risks of financial harm common to all forms of identity theft, the thief's medical history may be added to the victim's medical records. Inaccurate information in the victim's records is difficult to correct and may affect future insurability or cause doctors relying on the misinformation to deliver inappropriate medical care.

Child Identity Theft

Child identity theft occurs when a minor's Social Security number is used by another person for the imposter's personal gain. The imposter can be a family member, a friend, or even a stranger who targets children. The Social Security numbers of children are valued because they do not have any information associated with them. Thieves can establish lines of credit, obtain driver's licenses, or even buy a house using a child's identity. This fraud can go undetected for years, as most children don't discover the problem until years later.

Techniques for Obtaining and Exploiting Personal Information for Identity Theft

Identity thieves typically obtain and exploit personally identifiable information about individuals, or various credentials they use to authenticate themselves, in order to impersonate them. Examples include:

- Rummaging through rubbish for personal information (called "dumpster diving").
- Retrieving personal data from redundant IT equipment and storage media including PCs, servers, PDAs, mobile phones, USB memory sticks and hard drives that have been disposed of carelessly at public dump sites, given away or sold without having been properly sanitized.
- Using public records about individual citizens, published in official registers such as electoral rolls.
- Stealing bank or credit cards, identification cards, passports, or authentication tokens, typically by pickpocketing, housebreaking or mail theft.
- Common-knowledge questioning schemes that offer account verification and compromise: "What's your mother's maiden name?", "What was your first car model?", or "What was your first pet's name?" etc.
- Skimming information from bank or credit cards using compromised or hand-held card readers, and creating clone cards.
- Using 'contactless' credit card readers to acquire data wirelessly from RFID-enabled passports.

- Observing users typing their login credentials, credit/calling card numbers etc. into IT equipment located in public places (called “shoulder surfing”).
- Stealing personal information from computers using breaches in browser security or malware such as Trojan horse keystroke logging programs or other forms of spyware.
- Hacking computer networks, systems and databases to obtain personal data, often in large quantities.
- Exploiting breaches that result in the publication or more limited disclosure of personal information such as names, addresses, Social Security number or credit card numbers.
- Advertising bogus job offers in order to accumulate resumes and applications typically disclosing applicants' names, home and email addresses, telephone numbers and sometimes their banking details.
- Exploiting insider access and abusing the rights of privileged IT users to access personal data on their employers' systems.
- Infiltrating organizations that store and process large amounts of particularly valuable personal information.
- Impersonating trusted organizations in emails, SMS text messages, phone calls or other forms of communication in order to dupe victims into disclosing their personal information or login credentials, typically on a fake corporate website or data collection form (phishing).
- Brute-force attacking weak passwords and using inspired guesswork to compromise weak password reset questions.
- Obtaining castings of fingers for falsifying fingerprint identification.
- Browsing social networking websites for personal details published by users, often using this information to appear more credible in subsequent social engineering activities.
- Diverting victims' email in order to obtain personal information and credentials such as credit cards, billing and bank/credit card statements, or to delay the discovery of new accounts and credit agreements opened by the identity thieves in the victims' names.
- Using false pretenses to trick individuals, customer service representatives and help desk workers into disclosing personal information and login details or changing user passwords/access rights (pretexting)
- Stealing checks to acquire banking information, including account numbers and bank routing numbers.
- Guessing Social Security numbers by using information found on Internet social networks such as Facebook.
- Low security/privacy protection on photos that are easily clickable and downloaded on social networking sites.
- Befriending strangers on social networks and taking advantage of their trust until private information is given.

Individual Identity Protection

The acquisition of personal data is made possible through serious breaches of privacy. For consumers, this is usually a result of them naively providing their personal information or login credentials to the identity thieves.

Identity theft can be partially mitigated by *not* identifying oneself unnecessarily (a form of information security control known as risk avoidance). To protect against electronic identity theft by phishing, hacking or malware, individuals should maintain computer security, for example by keeping operating systems and web browsers security fully patched against known security vulnerabilities, running antivirus software and being cautious in their use of IT.

To protect themselves against identity theft, individuals are advised the following:

- Do not give out personal information (such as one's SSN) on the phone, fax or on social media platforms.
- Use a shredder to destroy tax related documents after tax time is over and keep the necessary ones in a safe (thieves can look through the trash).
- For taxpayers planning to e-file their tax returns, it is recommended to use a strong password. Afterwards, save the file to a CD or flash drive and keep it in a secure location. Then delete the personal return information from the computer hard drive.
- Only show employers your Social Security card at the start of a job, but otherwise do not routinely carry the card or other documents that display their SSN. Additionally, it is recommended not to fill the Social Security number on medical forms and such documents (in case your wallet or purse gets stolen).
- Only use secure websites while making online financial transactions (thieves access information you provide to an unsecured Internet site).
- If working with an accountant or tax professional, query him/her on what measures they take to protect your information.

Identity thieves sometimes impersonate recently deceased persons, using personal information obtained from death notices, gravestones and other sources to exploit delays between the death and the closure of the person's accounts, the inattentiveness of grieving families and weaknesses in the processes for credit-checking. Such crimes may continue for some time until the deceased's families or the authorities notice and react to anomalies.

In recent years, commercial identity theft protection/insurance services have become available in many countries. These services purport to help protect the individual from identity theft or help detect that identity theft has occurred in exchange for a monthly or annual membership fee or premium. The services typically work either by setting fraud alerts on the individual's credit files with the three major credit bureaus or by setting up credit report monitoring with the credit bureau. While identity theft protection/insurance services have been heavily marketed, their value has been called into question.

Responses to Identity Theft

1. The ID Theft victim should place a fraud alert on their credit report and obtain a copy of their credit report by contacting one of these credit reporting agencies (CRAs). The victim should not rely on one CRA to notify the other two; instead, he/she should contact all three CRAs:

- TransUnion: (800) 680-7289; **www.transunion.com**
- Equifax: (800) 525-6285; **www.equifax.com**
- Experian: (888) 397-3742; **www.experian.com**

2. Close compromised accounts immediately. The victim should contact every credit card company, bank or other financial institution where an account has been tampered with or opened fraudulently. He/she should review their credit reports for additional fraudulent accounts and close them where necessary. Follow-up should be done in writing.

3. Report the identity theft to the Federal Trade Commission: **www.ftc.gov/idtheft** or 1-877-ID-THEFT. The process involves completing an online complaint form, which can be used when filing a police report.

4. File a police report. The victim should attach a copy of the FTC complaint to the police report. It's also good to obtain a copy of the police report for safekeeping.

Other Self-Protection Steps

Monitor

Everyone should obtain a copy of their credit report periodically and review carefully. Each person has the right to one free credit report each year from each credit reporting agency. To request a copy of your credit report, go to **www.annualcreditreport.com**. For those who are actual identity theft victims, monitoring is crucial.

Monitoring should also be done of Social Security records. It is possible to request a copy of one's Social Security statement to determine if there is an irregularity in earnings reports.

Seven-year Fraud Alert

ID Theft victims can place a seven-year extended fraud alert on their credit report. This requires providing a copy of the identity theft report and providing current contact information. The credit reporting companies will put the contact information on the extended fraud alert to tell potential creditors they must contact the victim before issuing credit in his/her name.

Credit Freeze

Minnesota law allows an identity theft victim to place a freeze on their credit report. A credit freeze prevents the credit reporting agency from releasing a consumer's credit report or any information from it without the consumer's express authorization. To place a credit freeze, victims must request a freeze from each of the three nationwide credit reporting agencies. An

identity theft victim can obtain a freeze for free; others have to pay $5 to request a freeze. (Under Minnesota law, you can request a credit freeze even if you haven't been the victim of identity theft.) If the freeze requestor later wishes to obtain credit, he/she will need to arrange to "unfreeze" the credit.

Referrals for Specific Identity Theft Issues

Reporting lost or stolen social security cards:
For information regarding lost or stolen social security cards, go to the Social Security Administration Website (**www.ssa.gov**) or call 800-772-1213. Additional information can be found on the Deter Detect Defend Website (**www.ftc.gov/idtheft)** if you think your social security number has been misused.

If a Minnesota driver's license or identification card has been taken:
Persons whose license or state ID card has been stolen or used improperly will need to get a replacement at a local driver's license office. They can complete a **form** to request a "driving record flag" that will alert law enforcement officers that someone else may be using that person's identity. For more information, contact the Minnesota Department of Public Safety Driver and Vehicle Services at (651) 297-3298, or **dvs.dps.mn.gov**.

In Minnesota, the victim's local law enforcement agency is required to take a report regardless of where the crime occurred.
Victims should file a police report with the law enforcement agency where they live. Under Minnesota law, your local law enforcement agency *must* take a report of identity theft even if the suspected perpetrator is located and/or the ID theft occurred in another jurisdiction. The law enforcement agency is required to provide the victim a copy of it. This report will be helpful for the victim to provide to creditors who want proof of the crime. That agency can begin an investigation or refer the case to another jurisdiction if the suspected crime was committed in a different jurisdiction. Minn. Stat. § 609.527

In Minnesota, victims of identity theft are entitled to crime victim rights that accrue under Chapter 611A with an additional right to mandatory restitution:
In cases where the crime of identity theft is charged, victims are entitled to a mandatory restitution award of $1,000 as well as the ability to get free copies of court documents to aid in clearing up their personal credit and criminal histories without accumulating more costs. See Minn. Stat. § 609.527.

If someone's name has been used in a criminal case:
If someone has represented themselves as another person in a criminal prosecution, the victim can contact the Bureau of Criminal Apprehension (BCA) to question the identity on the criminal record. See the **BCA Website** (bca.dps.mn.gov) or call 651-793-2400. At the time of making a report, the victim can also request that his/her name be submitted to the FBI's **NCIC Identity**

Theft File, which provides a means for law enforcement to flag stolen identities and identify imposters when they are encountered.

For stolen passports, immigration, or citizenship documents:
For lost or stolen U.S. passport, naturalization, or citizenship certificate, contact the U.S. Citizenship and Immigration Services. For information go to the **USCIS Website** (**www.uscis.gov**) or call 1-800-375-5283. To replace a green card, see the **USCIS Website**. For information about lost or stolen passports, visas, or arrival/departure records, see the U.S. Department of State Website (**travel.state.gov**) for information. If someone is not a United States citizen, they must contact their consulate to replace their passport. Some consulates will request a law enforcement report.

Reporting phone, mail, or email fraud:
To report phone, mail, or email fraud, go to the Minnesota Fraud Enforcement Partnership at **www.mnscams.org** or call 866-347-0911. In addition, internet crimes can be reported to the Internet Crime Complaint Center (IC3): **www.ic3.gov**.

Victim Rights under Federal Law:
There are a number of federal laws designed to protect victims of identity theft. These laws are designed to assist victims in minimizing and repairing the harm done after being victimized. These laws address documenting the theft; dealing with credit reporting companies; dealing with creditors, debt collectors, and merchants; and limiting financial losses caused by the theft. A list of these rights can be found on the **Deter Detect Defend** Website: **www.ftc.gov/idtheft**.
FOR FURTHER ASSISTANCE: Crime Victim Justice Unit, Office of Justice Programs, 651-201-7310 | 800-247-0390 ext. 3, ojp.dps.mn.gov

IDENTITY THEFT RESOURCES

1. **Minnesota Attorney General Office 651-296-3353; 1-800-657-3787 (www.ag.state.mn.us).** The Attorney General's Office reports that it wants to hear from citizens about any identity theft or consumer fraud scam of any kind. They answer the telephone with a "live" person who can provide information and can make referrals. The **Minnesota Office of Attorney General** has several helpful guides on its website: **www.ag.state.mn.us :**
   Guarding Your Privacy: Tips to Prevent Identity Theft
   Consumer Alert: What to do When your Personal Information Has Been Breached
   Minnesota Identity Theft Freeze Law

2. **The Federal Trade Commission (1-877-FTC-HELP) and its Deter Detect Defend** website is the best source of information about what to do if one's personal information has been used or is at risk of being used: **Deter Detect www.ftc.gov/idtheft Defend** Website: **www.ftc.gov/idtheft**

Reporting a crime to the FTC Website will not necessarily prompt an investigation of the crime. The report is primarily used to track the incidence of ID theft and crime trends and may prompt an investigation or assist in an ongoing investigation, However, it should not be expected that a report will automatically lead to a criminal justice response. **Identity Theft Victims should always report the crime to their local law enforcement agency.**

3. The **Privacy Rights Clearinghouse and the Identity Theft Resource Center** have very useful information for dealing with identity theft:
   Privacy Rights Clearinghouse Identity Theft Resource Center
   www.privacyrights.org | (619) 298-3396 **www.idtheftcenter.org** | (888) 400-5530

Help for Zoey

Once again, Zoey's got a mess on her hands. Once more, she's been too trusting of others (but we love it that Zoey has a trusting nature). She's obviously got a problem that needs immediate attention. Of course, she should contact the Attorney General's office to report the identity theft. Similarly, she needs to file a police report. Then, she needs to place a freeze on her credit report with each of the three credit bureaus. Finally, she needs to contact **Detect Deter Defend** at the FTC website.

Unfortunately, it will take much time—maybe a year or more—for Zoey to sort out this mess. Certainly, she needs to make sure to answer any lawsuit with which she is served. Most of all, she has to persevere. This is something that Zoey, our heroine, is good at.

This Month's Tips

1. **Remember that Legal Aid and VLN won't handle personal injury or property damage claims. They are, for the most part, dedicated to handling legal matters involving the Five Core Risk Areas—shelter, safety, health, employment benefits (such as unemployment insurance), and key family relationships (child custody and establishing support obligations). If you get a call from someone who might have the ability to recovery money from someone else as the result of an accident or business dispute, then refer the caller to the private bar (such as the HCBA Lawyer Referral & Information Service and the RCBA Attorney Referral Service).**

Let us know if you have any questions!

ellie and Jillian